

Security Management Introduction

Arquitectura de servidores con software libre

GSyC

Pedro Coca

pcoca@libresoft.es

1st April 2011

we study libre software

GSyC



Universidad
Rey Juan Carlos

GSyC

LibreSoft

(cc) 2011 Pedro Coca.

This presentation is published under the Creative Commons 3.0
Attribution, available at

<http://creativecommons.org/licenses/by/3.0/>

Security Management: Introduction

- Primary Concepts: C-I-A
- Confidentiality: Information Classification
- Integrity: Data cannot be altered without being detected
- Availability: Fault tolerance, Single point of failure, backups, etc.

GSyC

we study libre software

Security Management: Introduction

- Security is a comprehensive area, including:
 - Risk Management
 - Information Security Policies
 - Guidelines, Baselines, Procedures and Standards
 - Security organisation and education, etc
- The aim of security is to protect the company/entity and its assets

Security Management: Concepts

- **Identification:** means by which users identify themselves to the system
- **Authentication:** testing or reconciliation of evidence of users identity
- **Accountability:** system ability to determine actions of users within the system and identify the user
- **Authorisation:** rights and permissions granted to a user or process
- **Privacy:** Level of confidentiality and privacy protection of a user

Before talking more about security...

- Libre software and Security
- More or Less secure?



Security in Libre Software: Myths and facts

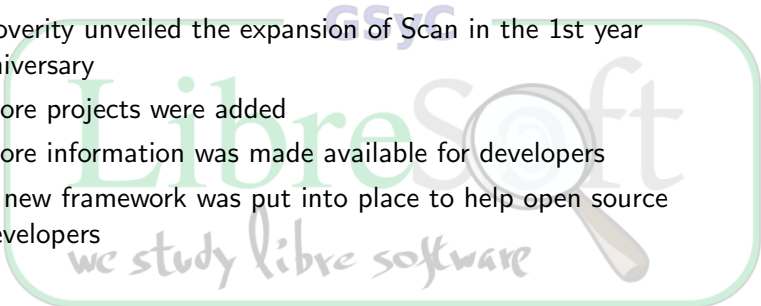
- Is Open Source Good for Security?
<http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html>
- Risky business: Keeping security a secret
<http://www.zdnet.com/news/risky-business-keeping-security-a-secret/127072>

FLOSS Security: facts

- Coverity Scan Initiative
- Launched on March 6, 2006
- In the first year of operation, over 6,000 software defects were fixed
- FLOSS developers use the analysis results from the Coverity Scan service
- In the first year, 50 open source projects written in C and C++ were included.

Coverity Scan

- Coverity unveiled the expansion of Scan in the 1st year anniversary
- More projects were added
- More information was made available for developers
- A new framework was put into place to help open source developers



Coverity Scan 2010

- Coverity Scan 2010 experiment another transformation
- Up to 291 projects
- 191 out of 291 with active developer support
- Over 61 million unique lines of code were tested
- 49.654 defects identified
- ... and the open source community has fixed 15.278 of them.

Coverity Scan 2010. Defects

TABLE 2: MOST COMMONLY FOUND DEFECTS

Defect Type	2008 Frequency	2009 Frequency	2010 Frequency	% Difference from 2009	Risk/Impact Category
NULL Pointer Dereference	27.95%	27.81%	27.60%	0.19% ↓	Medium
Resource Leak	25.73%	23.34%	23.19%	0.15% ↓	High
Unintentional Ignored Expressions	9.76%	9.71%	9.76%	0.05% ↑	Medium
Use Before Test (NULL)	8.09%	8.35%	8.86%	0.51% ↑	Medium
Uninitialized Values Read	5.50%	8.41%	8.30%	0.09% ↓	High
Use After Free	6.46%	5.91%	5.64%	0.27% ↓	High
Buffer Overflow (statically allocated)	6.14%	5.79%	5.52%	0.27% ↓	High
Unsafe Use of Returned NULL	5.85%	5.30%	5.37%	0.07% ↑	Medium
Unsafe Use of Returned Negative	3.72%	3.90%	3.73%	0.17% ↓	Medium
Type and Allocation Size Mismatch	.62%	1.10%	1.56%	0.46% ↑	High
Buffer Overflow (dynamically allocated)	.31%	.21%	.29%	0.08% ↑	High
Use Before Test (negative)	.21%	.18%	.17%	0.01% ↓	Medium

Coverity Scan. Integrity Levels

- Coverity Integrity Level 1
 - Defect density equals or less than 1 defect/kloc
- Coverity Integrity Level 2
 - Defect density equals or less than 0.1 defect/kloc
 - 90th industry percentile
- Coverity Integrity Level 3
 - Defect density equals or less than 0.01 defect/kloc (99th industry percentile)
 - Less than 20 % of the results
 - Zero high defects
- Level Not Achieved
 - Too many unresolved defects

Coverity Scan 2010

- Several popular projects (Firefox, Linux and PHP) were included before
- Android kernel 2.6.32 (Froyo) was included in 2010
 - Lines of Code Inspected: 765,642
 - Project Defect Density: 0.47 (defects per thousand lines of code)
 - High and Medium Impact Defects: 359

Coverity Scan 2010: Android Froyo

High-Risk Defects

High-impact defects that cause crashes, program instability, and performance problems.

Memory - corruptions

20

Memory - illegal accesses

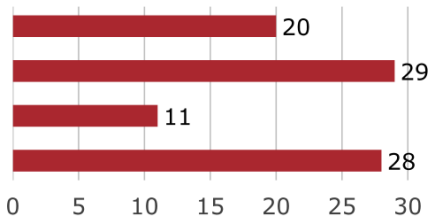
29

Resource leaks

11

Uninitialized variables

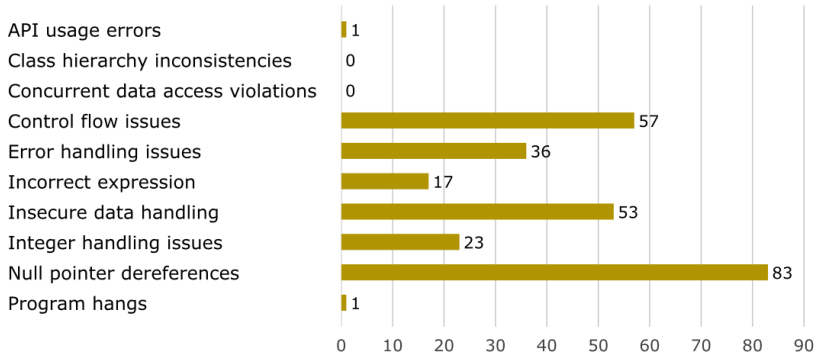
28



Coverity Scan 2010: Android Froyo

Medium-Risk Defects

Medium-impact defects that cause incorrect results, concurrency problems, and system freezes.



Coverity Scan 2010: Android Froyo

- The Android kernel used in the HTC Droid Incredible has approximately half the defects that would be expected for average software of the same size.
- Android-specific code that differs from the Linux kernel had about twice the defect density of the core Linux kernel components.

we study libre software

Coverity Scan

- For more information and details, check out the 2008, 2009 and 2010 reports.

Questions? / Comments?

we study libre software

Risk Management: Introduction

- The aim of security is to protect the company/entity and its assets
- Risk management
 - Identifies these assets
 - Point to the threats putting them in peril
 - Estimates the potential loss and harm if the threat becomes reality
 - Identify action plans to mitigate those risks
 - Provide an economic balance between the safeguard implemented and the impact of the threat

Security Management: Definitions

- Vulnerability
 - Absence or weakness of a safeguard
 - Is a HW or SW weakness that may provide an attacker a way to compromise our (CIA) system.
 - Could be an open port, unpatched applications, unrestricted modem dial-in access, no physical security, etc,
- Threat
 - Any event that causes an undesirable impact on our organisation.
 - Any potential danger to the system or to the information.
 - Could be a Tsunami, an unintentional mistake leading to confidential data exposure, a process reading data violating our data policy, etc

Security Management: Definitions

- Risk
 - Is the probability of a threat agent exploiting a vulnerability and the corresponding business impact
 - Potential lost or harm to a system.
 - If there is no IDS, the risk (likelihood) of unnoticed attacks would be high
 - If there is no awareness training, the risk of unintentional mistakes causing information deletion/exposure would be high
- Exposure
 - Is an instance of being exposed to harm or lost from an entity that takes advantage of a vulnerability

Security Management: Definitions

- Safeguard
 - Is the countermeasure to put in place to mitigate the potential risk
 - Could be a procedure, a piece of HW or SW, etc
 - Access Controls, strong password management policies, awareness training, etc

GSyC

we study libre software

Security Management: Risk Management

- Information Risk Management (IRM)
 - The prime objective of security controls is to reduce effects of threats and vulnerabilities to a level that is tolerable
 - We have to implement the right mechanism to set and keep that level of risk
- Types of Risk
 - There are many risk categories: Physical damage, Human interaction, Equipment malfunction, Inside and outside attacks, Misuse of data, Loss of data and Application errors.

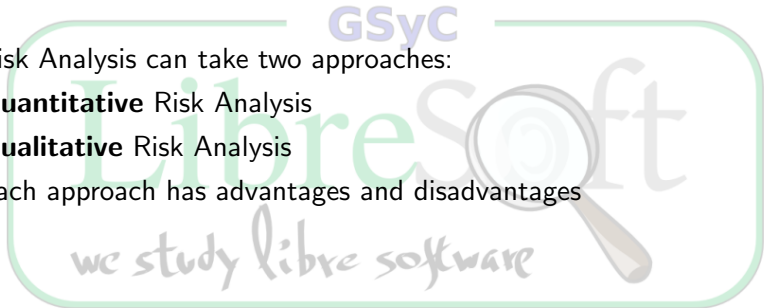
Security Management: Risk Analysis

- Risk Analysis Objectives

- Identify assets and their values
- Identify vulnerabilities and threats
- Quantifying the probability and business impact of these potential threats
- Provide an economic balance between the impact of the threat and the cost of the countermeasure

Security Management: Risk Analysis

- Risk Analysis can take two approaches:
- **Quantitative** Risk Analysis
- **Qualitative** Risk Analysis
- Each approach has advantages and disadvantages



Security Management: Risk Analysis

- Risk Analysis Steps

- Assign Value to Assets
- Estimate potential loss per threat
- Carry out a threat analysis
- Derive the Overall Loss Potential per Threat
- Reduce, Transfer or Accept the risk

GSyC

we study libre software

Security Management: Risk Analysis

- Value of Assets
 - Quantitative and Qualitative measures
 - The actual value of an asset is determined by the cost to acquire, develop and maintain it.
 - Value of the asset to owners and users
 - Value of the asset to competitors
 - Intellectual property issues
 - Liability issues (Data protection)
 - It is critical to take into account the business impact!

Security Management: Risk Analysis

- Identifying Threats

- Viruses, Attacks, Intruders
- Physical Threats
- Employees / Users / Contractors
- Gather information about the probability of each threat
- Calculate the annualised rate of occurrence (ARO)

GSyC

we study libre software

Security Management: Risk Analysis

- Reduce, Transfer or Accept the Risk
 - Reducing the risk:
 - Set controls
 - Improve procedures
 - Security awareness training
 - ...
 - Transferring the risk:
 - Insurance
 - Accepting the risks:
 - Stop using resources for protection and live with the risk

Security Management: Risk Analysis

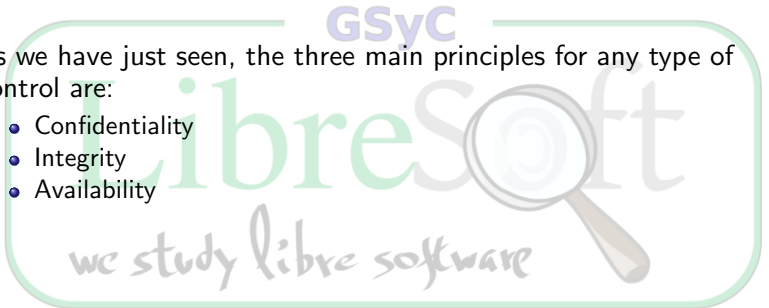
- Risk Analysis Results
 - Monetary values assigned to assets
 - Comprehensive list of all possible and significant threats
 - Likelihood of the occurrence rate (for each threat)
 - Potential loss that the company/entity can endure per threat in a timely basis
 - Recommended safeguards, remediation actions, countermeasures
- Residual Risk

Access Control Definition

- Set of procedures performed by hardware, software and administrative items
- Aimed to:
 - Monitor access
 - Identify user requesting access
 - Record access attempts
 - Grant or deny access based on a pre-established rules

Access Control Principles

- As we have just seen, the three main principles for any type of control are:
 - Confidentiality
 - Integrity
 - Availability



Access Control Models: MAC

- Mandatory Access Control
 - Subjects have a **clearance**
 - Objects have a **classification**
 - Subjects must have a **need to know** over the Objects
 - Subjects can access Objects with the same or below clearance level and a need to know for the Objects
 - Rule-based access control is a type of MAC (access is not based on identity)
 - Unclassified, confidential, secret and top secret **sensitivity**
 - SELinux, TrustedBSD are examples of Free OS implementing MAC

Access Control Models: DAC

- Discretionary Access Control
 - The subject can specify (with limitations) what objects are accessible
 - Access Control Lists (ACL) can be set up
 - ACL shows what subjects can use what objects with what privileges
 - Common Unix system of users, groups, and read-write-execute permissions
 - Identity-based access controls

Access Control Models: Non DAC

- Non-Discretionary Access Control
 - Also known as Role-based access control (RBAC)
 - Assigning a user to a role is imposed (Always)
 - A central Authority determines access between subjects and objects
 - Access controls can be role-based or task-based
 - These kind of control do not need to be updated if there is a role change in the company
 - is RBAC a type of MAC?
 - <http://csrc.nist.gov/rbac>

Access Control Models Wrap up

- **MAC:** Operating Systems, using security labels, enforce the model and therefore their security system
- **DAC:** Data owners decide which subjects has access to which objects
- **RBAC:** Access to objects is determined by the role of each subject

Access Control Types

- Preventive (Inhibit)
- Detective (Discover)
- Corrective (Restoring)



Access Control Implementation

- Access Controls can be implemented with a set of measures:
 - **Administrative**
 - Policies, procedures, staff training, reviews.
 - **Logical/Technical**
 - ACL, Firewalls, Smart Card Access, Encryption, etc
 - **Physical**
 - Server Facilities locking, backing up, cable protection, etc

Access Control Attacks

- Denial of Service
 - Compromises the availability
 - Buffer Overflows, SYN Attack, etc
 - Authorisation
- Back Door
 - Bypasses access control mechanisms
- Spoofing, Man in the Middle, Session Hijacking, Social Engineering.
- Dumpster diving
- Password guessing, Brute Force, Dictionary Attacks
- Software exploits, Trojan Horses, etc

Access Accountability

- Access Controls provide Access Accountability
- Access Accountability needs:
 - Identification
 - Authentication
 - Authorisation



Identification, Authentication and Authorisation

- **Identification** sets a method of ensuring that a user, program or process (any subject) is the entity it claims to be.
 - Usernames, Account numbers are ways to identify a subject
- **Authentication** is the fact of confirming an identity claim made by or about the subject
 - Passwords, PINs, Criptographic key, etc are usually authentication methods
- **Authorisation** is the procedure of specifying access rights to a set of resources
 - Usually the system checks an access control matrix or an ACL

Strong Authentication

- There are 3 general aspects to prove be authenticated:
 - Something you **KNOW**
 - Usually a PIN, password, etc
 - Easy and cheap to implement
 - Something you **HAVE**
 - Usually a key, a badge, etc
 - Normally used for physical access, but can be required for logical access
 - Something you **ARE**
 - Biometrics
 - Complex and expensive implementation.
 - False positives/negatives (Type I/II errors). Crossover rate
- **Strong Authentication** contains 2 out of 3 aspects. Also know as **two-factor authentication**

Passwords

- Most common authentication method: User id bound with a reusable password.
- Also weakest method!
- Therefore, usually access control relies on password strength
- Becomes very important the password management policy
- Is an important target in attacks
- Tools to analyse the targeted social network profiles to create custom dicts
- Tools to create non-dictionary typical human variations

Password gathering techniques

- Monitoring
- Accessing the password file
- Brute force attacks
- Dictionary attacks
- Social engineering



Password protection measures

- Set a clipping Level (user will be locked out for a fixed time)
- Limit the number of failed logon attempts
- Awareness training
- Password checkers
- Password hashing and Encryption
- Password aging
- Cognitive passwords
- One-Time passwords (dynamic passwords)
- Token devices
 - Synchronous
 - Asynchronous (challenge/response)

Access Control Assignment

- Password strength audit
- Using a well known GPL password cracker: John the ripper
- Add test users with increasing password complexity
- Perform a password strength audit in your own system
- Measure the time needed to crack the password with the password complexity

Access Control Assignment

- Download John the ripper software
- Download "SHA-512" patch, so hashes can be loaded (Recent Ubuntu and Fedora)
- Apply the patch and compile the patched john source code
- Unshadow the password file
- Proceed to audit the file

Access Control Assignment

- Of course, there are other good alternatives password audit FLOSS:

- **THC Indra**
- <http://www.thc.org/thc-hydra/>
- **Aircrack**
- <http://www.aircrack-ng.org/>
- **Airsnort**
- <http://airsnort.shmoo.com/>

John the ripper: GPL Password Audit Tool screenshot

GSyC

```
pcoca@chipiron:~/john-1.7.3.1/run$ sudo ./unshadow /etc/passwd /etc/shadow > crack.me
pcoca@chipiron:~/john-1.7.3.1/run$ ./john crack.me
Loaded 10 password hashes with 10 different salts (generic crypt(3) [?/32])
test1 (test1)
test2 (test2)
abc (test3)
butterfly (test9)
dontknow (test8)
maria (test5)
guesses: 6 time: 0:00:17:22 7% (2) c/s: 47.01 trying: cookie1
```

we study libre software

Access Control Questions

GSyC
LibreSoftware
we study libre software

How can the cheap and easy access to compute power in the cloud change the access control landscape?

Access Control Questions

- Cloud Cracking Suite presentation at Black Hat EU 2011:
 - https://stacksmashing.net/stuff/bh_eu_2011.pdf
- Cracking Passwords In The Cloud: Amazon's New EC2 GPU Instances
 - <http://stacksmashing.net/2010/11/15/cracking-in-the-cloud-amazons-new-ec2-gpu-instances/>
- Researcher uses AWS cloud to crack Wi-Fi passwords
 - <http://www.zdnet.co.uk/news/cloud/2011/01/14/researcher-uses-aws-cloud-to-crack-wi-fi-passwords-4009>

Questions?

